

REMARKS

In this Amendment, claims 21, 24 and 32-36 have been amended, and new claims 39 and 40 added. Care has been exercised to avoid the introduction of new matter. Specifically, adequate descriptive support for the amendments of the claims can be found on, for example, page 12, line 4 to page 14, line 2; page 17, lines 6-10; page 18, line 23 to page 19, line 4; and page 20, lines 13-22 of the specification. New claims 39 and 40 are the same as those presented in the July 27, 2006 Amendment, but not entered (see paragraph 1 of the August 22, 2006 Advisory Action).

Now, claims 21, 24-36, 39 and 40 are active in this application, of which claims 1, 32-36, 39 and 40 are independent.

Claims 21-38 have been rejected under 35 U.S.C. §102(e) as being anticipated by Rabin et al.

In the statement of the rejection, the Examiner asserted that Rabin et al. discloses methods and apparatus for protecting information identically corresponding to what is claimed. It is noted that the rejection of claims 22 and 23 has been rendered moot by cancellation of these claims.

Applicants submit that Rabin et al. does not disclose a recording and reproducing device including all the limitations recited in independent claim 21, as amended. Specifically, Rabin et al. does not disclose, among other things, the following limitations in claim 21:

an abuse prevention information calculating unit operable to calculate

a) first abuse prevention information at the time of powering off the recording and reproducing device, by performing a specific function on the control program stored in the program storage unit, and

b) second abuse prevention information at the time of powering on the recording and reproducing device, by performing the specific function on the control program stored in the program storage unit;

a comparing unit operable to compare, if necessary, the first abuse prevention information stored in the abuse prevention information storage unit and the second abuse prevention information calculated at the time of powering on the device, and then judging the abuse based on the comparing result.

The present invention is configured to detect alteration of the control program, the alteration made while the device is powered off. In a well-known modification (tampering) of a recording and reproducing device, an HDD is removed from the device at the time of power-off, analyzed and tampered, and then, is attached again to the device. The present application addresses protection of the device against such tampering.

Applicants submit **Exhibit A** to explain differences between the present invention and Rabin et al. As shown in **Exhibit A**, in the present invention, first abuse prevention information on a control program is calculated at the time of powering off the recording and reproducing device. Second abuse prevention information on the control program is also calculated at the time of powering on the device, and the first abuse prevention information is compared with the second prevention information. If it is determined that the first abuse prevention information is different from the second abuse prevention information, the present invention recognizes that the abuse of the control program has occurred while the device is powered off. Therefore, the present invention can detect alteration of the control program made while the device is powered off.

Rabin's method and apparatus enables owners and vendors of software products to protect property rights of their software, in which a unique vendor tag system is utilized for each instant of a specific software product to detect unauthorized use or copy of the software (see the Abstract). Specifically, Rabin et al. neither discloses nor teaches calculating the abuse

prevention information at the time of powering off the apparatus. The Examiner explained what is disclosed in Rabin et al. in paragraph 5 of the August 22, 2006 Advisory Action, which is reproduced below (emphasis added):

Rabins calculates the abuse prevention information and stores it in the Non-volatile memory 200. This information is stored to detect the abuse at all time even after ten times of power off and on. The instance of software is installing, using, executing, running connecting with, reading, otherwise retrieving from a storage medium or modifying a storage medium. A hash of such instance is called tag, which is a true signature of the instance or even the software itself, wherein instance is modifying a storage medium (Col 30 lines 37-55). Before each usage of the software or periodically, the supervising program verifies that a valid tag exists (signature of software or instance) to ensure authenticity (Col 27 line 65 to Col 28 line 10). This verification process ensures the integrity of the software at all times and even prevents or detects unauthorized modification.

As acknowledged by the Examiner, Rabin et al. calculates a hash (Hash_INST_SW), for example, before a program is installed, and maintained the hash to compare it with a recalculated hash, determining whether there is an unauthorized modification on the program. **Exhibit A** depicts this process. It is noted that Rabin et al. does not recalculate the original hash (Hash_INST_SW), but uses it “at all the time even after ten times of power off and on,” as stated by the Examiner. Rabin et al. supports Applicants’ position in, for example, column 41, lines 18-28, and step 255 of Fig. 5. Tag Tag_INST_SW includes hash Hash_INST_SW, and is used to detect alteration of a program. Rabin et al. is silent on recalculation of hash Hash_INST_SW. It is also noted that step 277 “UPDATE TAG TABLE” in Fig. 8 does not mean recalculation of hash Hash_INST_SW. This step updates the status of tag Tag_INST_SW only (column 49, lines 3-7, see, also, Fig. 12 and column 54, lines 19-34).

In contrast, the claimed invention calculates first abuse prevention information on a control program at the time of the powering off the recording and reproducing device, in order to compare with second abuse prevention information on the control program to be calculated at the

time of powering on the device. Rabin et al. does not disclose calculating the first abuse prevention information at the time of powering of the device. Rather, Rabin et al. calculates a hash before a program is installed, and use it without any change.

Applicants further explain differences between the claimed invention and Rabin et al. Applicants invite the Examiner's attention to **Exhibit B**. Assuming that software allows part of its configuration (e.g., a configuration file) to be changed as a process proceeds, Rabin cannot detect whether the software has the latest configuration (including the configuration file), but can only detect whether it is the original. When an HDD in Rabin's system is removed and modified, changing part (the configuration file, for example) cannot be detected as tampering. The HDD can freely be modified in Rabin et al. In addition, Rabin et al. may determine an update of software as tampering even if it is authorized update. In contrast, the claimed invention requires calculating the abuse prevention information at the time of power-off, and uses that information to detect alteration of the control program controlling the recording and reproducing device, the alteration made while the device is powered off. Again, this requirement is not disclosed in Rabin et al.

In the second full paragraph at page 4 of the Advisory Action, the Examiner asserted that "[m]emory 200 [of Rabin et al.] is a non-volatile memory, which means that the information does not get erased when the power is off." As asserted by the Examiner, data in the non-volatile memory is not erased even when the power is off. However, this Examiner's assertion is irrelevant to the present invention. The present invention is for detecting the alteration of the control program that is made during the power-off of the recording and reproducing device. The present invention is configured so that the first abuse prevent information is calculated by using the function on the control program at the time of power-off of the recording and reproducing

device, and the second abuse prevent information is calculated at the time of power-on of the device. When the control program storage unit containing the control program is removed from the device to be tampered, or the control program storage unit is removed to be exchanged with other storage, the present invention can detect such tamper.

As discussed above, the present invention requires calculating the first abuse prevention information at the time of power-off of the recording and reproducing device, and comparing the first abuse prevention information and the second abuse prevention information. This requirement makes it possible to protect software including the above-described changeable part against tampering. In addition, this requirement avoids determining an authorized update as tampering, unlike Rabin's system.

Accordingly, Rabin et al. does not disclose a recording and reproducing device including all the limitations recited in independent claim 21, as amended. Dependent claims 24-31 are also patentably distinguishable over Rabin et al. at least because they respectively include all the limitations recited in independent claim 21. Applicants further note that the above discussion is applicable to independent claims 32-36, as amended.

Therefore, Applicants respectfully solicit withdrawal of the rejection of the claims under 35 U.S.C. §102(e) and favorable consideration thereof.

New claims 39 and 40 have been presented as replacement for claims 37 and 38. Applicants submit that Rabin et al. does not disclose a recording and reproducing device including all the limitations recited in new independent claim 39, as amended. Specifically, the reference does not disclose, at a minimum, that a control instruction sent from an abuse detecting server to a revoking unit in response to a notice of no abuse allows a recording and reproducing

device to be operated, and if no control instruction, the revoking unit halts the device after a specific time.

Rabin et al. teaches that abuse detection is notified to a server and then, operation of a user device is stopped. In Rabin's system, the tampered user device can be used if there is no connection between the tampered device and the server through a network. In contrast, the claimed invention can prevent an abuse of a control program controlling a recording and reproducing device without connection between the device and a server through a network. New claim 39 requires a revoking unit to "halt the use of the recording and reproducing device..." if no control instruction is sent from an abuse detecting server. In addition, Rabin et al. does not disclose allowing operation of the recording and reproducing device based on the control instruction from the abuse detecting server when no abuse is detected.

Accordingly, Rabin et al. does not disclose a recoding and reproducing device including all the limitations recited in independent claim 39. This discussion is applicable to new independent claim 40 reciting an abuse prevention system including a recording and reproducing device. Applicants, therefore, respectfully solicit favorable consideration of new claims 39 and 40.

Conclusion

It should, therefore, be apparent that the imposed rejections have been overcome and that all pending claims are in condition for immediate allowance. Favorable consideration is, therefore, respectfully solicited.

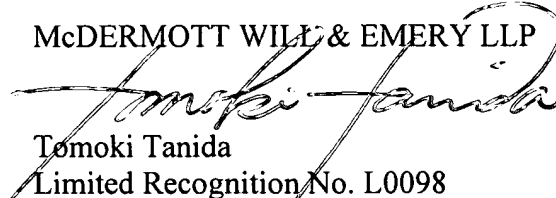
To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper,

Application No.: 10/092,472

including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Tomoki Tanida
Limited Recognition No. L0098

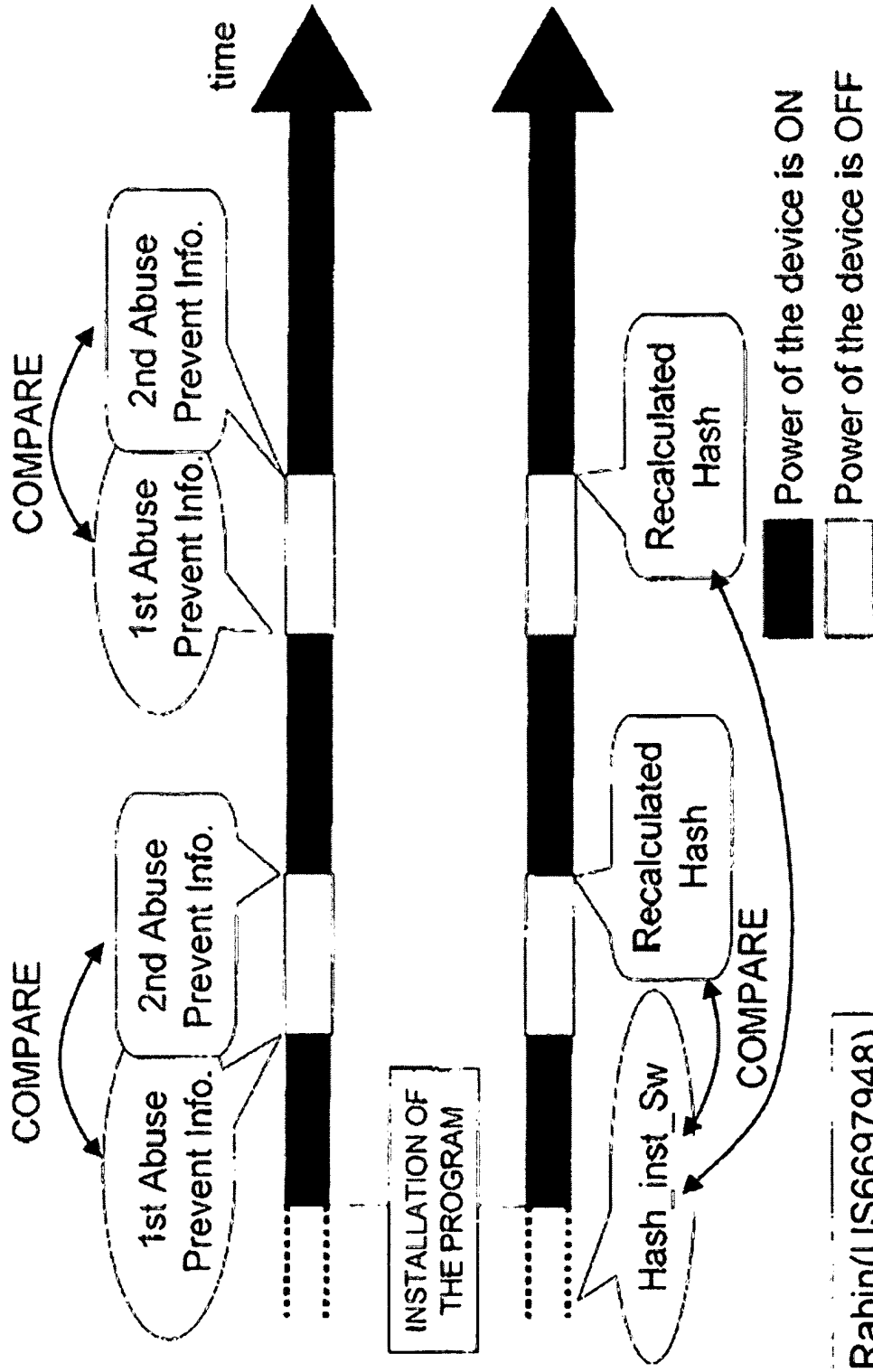
600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 SAB:TT
Facsimile: 202.756.8087
Date: September 28, 2006

**Please recognize our Customer No. 20277
as our correspondence address.**

WDC99 1287340-1.050023.0166

Exhibit A

Present Invention

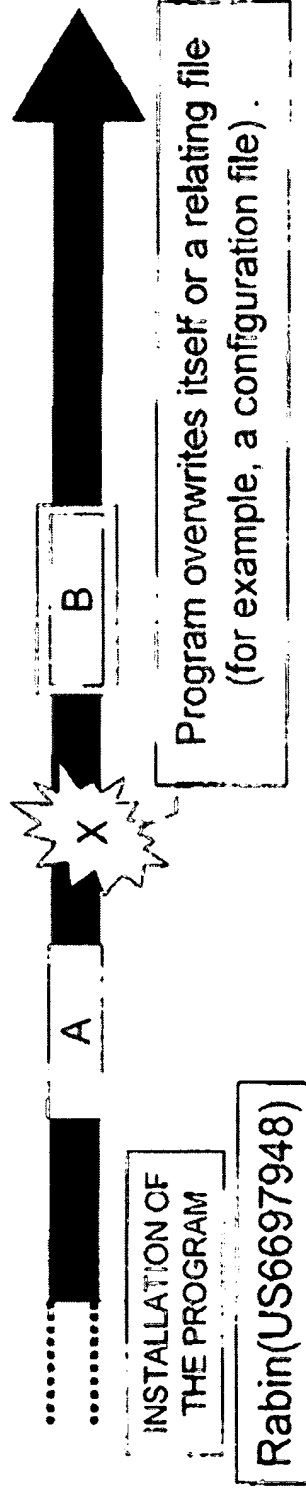


Rabin(US6697948)

※ Each balloon shows the timing at which the Info. or the hash is calculated.



Exhibit B



Rabin only stores the hash before the installation.

So, it can't detect abuse occurred in the section B completely.

As Rabin doesn't store a hash of the program after X,

Rabin's stored hash doesn't reflect new features arisen at X.

So, Rabin can't detect abuse about the new features.

Present Invention

The present invention calculates 1st abuse prevention

at the timing of power-off (strictly speaking, just before the power-off).

So, the present invention CAN detect the abuse in the section B completely.

As the 1st abuse prevent information is calculated at the power-off timing of the section B (i.e. the left edge of the section B), the 1st abuse prevent information can fully reflect the new features arisen at X.